1415 N CHERRY AVE
CHICAGO, IL 60642
(312) 281-6900
DMDII.ORG
DMDII@UILABS.ORG

DMDII
a UI LABS Collaboration
DIGITIZING AMERICAN MANUFACTURING

DMDII FINAL PROJECT REPORT

Factory Operations Industrial Control Systems Cyber Security	
Principle Investigator / Email Address	Randall Sandone / rsandone@illinois.edu
Project Team Lead:	University of Illinois at Urbana-Champaign, Information Trust Institute
Project Designation	DMDII 15-01-02
UI LABS Contract Number	0220160015
Project Participants	University of Illinois at Urbana-Champaign Heartland Science and Technology Group Lockheed Martin HL Precision Manufacturing Integrity Technology Solutions
DMDII Funding Value	$235,938
Project Team Cost Share	$249,086
Award Date	13 June 2016
Completion Date	8 December 2017

This project was completed under the Cooperative Agreement W31P4Q-14-2-0001, between U.S. Army - Army Contracting Command - Redstone and UI LABS on behalf of the Digital Manufacturing and Design Innovation Institute. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of the Army.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The project team led by the Information Trust Institute at the University of Illinois at Urbana-Champaign and including Heartland Science and Technology Group, Lockheed Martin, HL Precision Manufacturing, and Integrity Technology Solutions assessed the cyber security posture and general level of knowledge of cyber security principles of a typical small/medium manufacturer. As a contractor subject to the DFARS, the SME contractor's level of compliance with DFARS 252.204-7012 was also assessed and an estimate of costs to reach full compliance was conducted.

[We feel it important to acknowledge upfront that the number of SMEs that were engaged in our project represented a statistically insignificant sample size given the large number of SMEs in the US manufacturing base. Nevertheless, an important aspect of our project was to document our observations and impressions as regards to the cybersecurity posture of the SMEs and their preparedness to comply with the DFARS. We cannot and do not assert that the observations and conclusions we present in this report are representative of the SME manufacturer base writ large. That said, we do believe that the observations and data contained herein adds value to the national dialog concerning the potential impact – both positive and negative – of the DFARS mandate.]

Our assessment of HL Precision, which was conducted in concert with its outsourced IT services provider Integrity Technology Solutions convinced us that the high level of anxiety and consternation regarding the potential cost and disruption to the Defense manufacturing base (particularly among SME manufacturers) that occasioned the release of the DFARS, was largely unwarranted. This perception was further buttressed by similar assessments of multiple SME manufacturers that participated in our beta test program. Contrary to the view that many have expressed, the SMEs that we assessed demonstrated a desire and willingness to improve their cybersecurity posture as a matter of sound business practice (irrespective of the DFARS). They demonstrated a desire to comply with the new DFARS requirement in order to protect their federal business base (even though in some cases that represented a modest fraction of their overall revenues) and to be positioned to secure additional federal business.

It was, however, obvious to us that much anxiety about DFARS compliance was the result of fear, uncertainty, and doubt. Uncertainty as to what precisely was required to comply with the DFARS led to fear that DFARS requirements were unattainable for an SME, and doubt that the SME would find compliance "affordable" vis-à-vis the potential loss of federal revenue. We came to the conclusion that if given a tool that would eliminate the confusion, minimize the cost, and accelerate compliance with the DFARS that most SMEs would pursue compliance both as a matter of sound business practice and to protect their federal revenues.

At the same time, the team was privy to results from other research being conducted at UIUC (funded by the Department of Homeland Security) that suggested that broader market forces – driven by the insurance industry and legal precedent – were driving businesses large and small to implement sound, *standardized*, cyber risk management policies and procedures. That research suggested that - irrespective of the DFARS - these market forces would soon exert pressure on SME manufacturers to improve their cybersecurity posture and risk management processes via *standardized* processes that could be recognized and accepted by insurers and courts as baseline reasonable and responsible

industry best practices. These same forces would likely compel prime contractors to enforce chain-wide conformance to such *standardized* practices to strengthen their supply chains and to minimize exposure to liabilities arising from losses caused by cybersecurity breaches at a supply chain member cascading to others or leading to contract quality or performance issues.

Based on this information, the team set out to build and deliver a tool that would: (1) help SME manufacturers comply with the DFARS and position their firms to address these emerging market forces and; (2) provide a sound platform to help prime contractors standardize cyber risk management within their supply chains and to provide a mechanism to monitor and validate conformance to the standard.

The team designed, developed, and tested a software application- the Cyber Secure Dashboard (the "Dashboard") - designed to allow SME manufacturers (and companies in many other industries) to achieve and maintain DFARS compliance and to meet a wide variety of cyber security requirements by implementing the cyber risk management process outlined in the NIST Cyber Security Framework.

The product was tested by multiple SME manufacturers within their own operational environments and feedback from the testing lead to improvements in the software and additional knowledge regarding the impact of the DFARS to SME manufacturers.

The Dashboard software and numerous reports and data have been delivered to DMDII on terms established in the DMDII Membership Agreement and grant award.

The Dashboard software is prepared for initial market release and a commercialization plan is being finalized that will ensure ongoing product development and support and sustainability of the product in the market.

Based on beta test feedback and general market feedback resulting from numerous product demonstrations the team believes that the Dashboard can significantly reduce the time, cost, and complexity of achieving and maintaining DFARS compliance and – depending upon market uptake – can significantly enhance the cybersecurity posture of the US manufacturing base.

II. PROJECT OVERVIEW

The overall objective of this project was to develop a baseline understanding of costs, capabilities, and effectiveness of DoD-required security measures for factory operations and to deliver solutions that would reduce the time and cost necessary to achieve compliance with those DoD-required security measures. Specific goals include:

- Identification of minimum capabilities that satisfy the requirements of DFARS 252.204-7012 for incorporating information security measures in a "typical" industry setting;
- Estimation of the costs to achieve and maintain those DFARS-compliant capabilities; and
- Development, test, and delivery of a solution which can advise manufacturing operations of their cybersecurity posture in general and their level of compliance with the DFARS specifically and to provide the resources necessary to achieve and maintain full compliance.

The team conducted an assessment of its SME partner (HL Precision Manufacturing) with the help of its outsourced IT services provider (Integrity Technology Solutions) to ascertain the general state of cyber

security awareness and preparedness at HL and to specifically assess its level of compliance with the DFARS. Informed by that knowledge the team developed a cloud-based Dashboard that serves as an easy tool to manage a company's cyber security posture and compliance process. In particular, the Dashboard serves as a unified resource for integrating a company's compliance efforts; for managing a company's implementation of security controls; for centralizing compliance artifacts; and for communicating compliance status to corporate managers and interested third parties (such as prime contractors, insurance companies, and government procurement officials).

Additionally, the Dashboard was designed to support compliance with the DFARS in a methodology that adheres to the NIST Cyber Security Framework risk management process. In doing so, the Dashboard not only supports specific compliance with the DFARS but also establishes the NIST CSF risk management process as the foundation for future growth in cybersecurity maturity for the company.

The Dashboard was beta-tested at four other SME manufacturers. The beta-test consisted of a four-phase approach:

(1) assessment of the cyber security awareness/posture of the SME which included a requirement-by-requirement assessment of the SME's state of compliance with the DFARS (NIST 800-171);

(2) training on the use of the Dashboard to manage the SME's cyber security compliance activities;

(3) use of the Dashboard by the SME to document and manage DFARS compliance activities;

(4) assessment of the costs of compliance activities during the beta program and estimate of full cost to comply with the DFARS.

Throughout the beta test the team received direct feedback regarding the efficacy of the Dashboard to meet the needs of SMEs to reduce confusion and to lower the cost and accelerate compliance with the DFARS. In addition, the beta test identified a number of software bugs and recommended enhancements to the Dashboard which have since been addressed by the team.

As more fully discussed below (see "Industry Impact & Potential") - based on beta test results and feedback from a wide range of sources - we believe that the Dashboard has the potential to become a de facto standard cyber risk management platform for both SME manufacturers and large-scale manufacturers as market forces converge to incentivize implementation and maintenance of *standardized* cyber risk management processes.

III. TECHNOLOGY OUTCOMES

CYBER SECURE DASHBOARD

The Dashboard is a cloud-based application that facilitates an organization's compliance with the DFARS 252.204-7012 and the NIST Special Publication 800-171r1. The Dashboard itself is a project management tool that tracks compliance; streamlines the compliance process; provides in-tool access to relevant documentation, best practices, and policy templates; provides a repository for compliance artifacts; and serves as a portal to cyber security references and tools available in the wider community via the web.

Several of the key benefits of the Dashboard design are:

- Its cloud-based design makes it easy to access, easy to use, and offers unlimited user access

- Fully integrates the NIST 800-171 requirements and NIST Cyber Security Framework in one platform
- Supports easy adaptation to NIST Cyber Security Profiles such as the Manufacturing Profile*
- Automates mapping of all relevant NIST 800 series documents and security controls
- Streamlines compliance with the DFARS and conformance to the NIST CSF cyber risk management process
- Provides a "birds-eye" view of compliance status and progress
- Supports a single site or multiple, potentially remote sites in one centralized platform
- Supports trusted third-party assessment/validation
- Supports corporate-wide engagement
- Provides in-tool access to all relevant documentation, best practices, and templates
- Serves as centralized repository for all compliance artifacts
- Serves as a portal to a world of resources available via the web

* Through a grant from the Department of Homeland Security, UIUC is in the process of enhancing the Dashboard to support the NIST Cyber Security Manufacturing Profile. This enhancement is scheduled to be released to the market in Q1 2018. With this enhancement, SME manufacturer users of the Dashboard will be able to comply with the DFARS, conform to the NIST CSF, and migrate to conformance to the Manufacturing Profile if and as needed.

The DHS project seeks to address the following **hypothesis**: *Prime contractors can facilitate a virtuous cycle by leveraging emerging market forces and new tools to incentivize their supply chains to conform to standardized cyber risk management processes (specifically the NIST Cyber Security Framework). This, in-turn, strengthens and accelerates those market forces to create further incentive on supply chain members to conform to the standard. This broad conformance – incentivized and facilitated by the virtuous cycle - will strengthen the cyber security and resilience of the manufacturing supply chains and the manufacturing sector writ large.*

Accordingly, the project will – in addition to enhancing the Dashboard software – engage with insurers, prime contractors, SMMs, and other stakeholders to test the hypothesis. This engagement will culminate in a workshop exploring the potential to create and sustain a virtuous cycle as hypothesized.

A technology overview of the Dashboard is given below.

a. System Overview

The Dashboard, designed and formatted to adhere to the NIST CSF cyber risk management process, cross references the DFARS-mandated control requirements of the NIST SP 800-171 r1 with the cybersecurity control standard, the NIST SP 800-53r4, and provides concrete, best-practices implementation guidance, in-tool templates and resources, and links to other cybersecurity resources available via the web. It is designed to overcome the challenges of complying with the NIST's cybersecurity controls by intuitively guiding the organization through the process of securing their information technology systems in accordance with the DFARS requirements and implementing and maintaining a cyber security risk management process which adheres to the NIST CSF.

b. System Requirements

The Dashboard can be accessed via its cloud portal at: http://www.cybersecureDashboard.com or as an application hosted on an organization's internal server.

- Cloud portal: requires a modern web browser such as Chrome, Edge, or Firefox.
- Hosted in-house: In addition to a computer with a modern web browser for the end user, this configuration requires a server to host the Cyber Secure Dashboard Docker containers. A 64-bit CPU with 4 or more cores is recommended. The OS must be 64-bit and can be Linux, Mac or Windows, provided that the server supports virtualization. The server should have a minimum of 4GB of RAM and 30GB of disk space. More disk space may be required if the artifacts that will be uploaded require a lot of space.

c. System Architecture

The Dashboard uses Docker volumes and containers to make it easy to install and port to cloud or corporate servers. The Dashboard consists of 4 Docker containers and 2 Docker volumes (for the database and artifact files). The volumes are hosted on the server, outside of the Docker containers, to facilitate backup and disaster recovery.

d. Features & Attributes

The Dashboard application includes many features, functions, and references to facilitate the compliance process and to ensure a long-term compliance posture. A few of the key features of the Dashboard are noted below.

- STREAMLINED COMPLIANCE
  - Clarity - One step at a time
  - The Dashboard provides a step-by-step process to implement the NIST SP 800-171r1 cybersecurity controls in the context of the standard-bearer NIST Cyber Security Framework.
- IN-TOOL DOCUMENTATION
  - A Deep Knowledgebase
  - The Dashboard offers easy access to all relevant documentation, cross-referenced & organized for both the seasoned professional as well as the non-initiated user.
- INDUSTRY BEST PRACTICES
  - Best Practices at your fingertips
  - The Dashboard provides a complete set of detailed instructions, templates, & references to implement the full set of NIST SP 800-171r1 cybersecurity controls.
- ENTERPRISE AWARENESS
  - Long-term Security
  - The Dashboard provides tools & templates to implement, manage, and communicate cybersecurity requirements to your entire enterprise: Security Officers, Engineers, Program Managers, Developers, Users, HR, Procurement, and C-Suite Executives.

e. Modes of Operations

The Dashboard can be hosted in the cloud or by organizations in-house, but the end-user experience is the same.

f. Software Development Documentation/Design Document

The Dashboard development efforts started by reviewing and assessing the existing government and commercial cyber security tools, reviewing the relevant NIST 800-series cyber security publications, and reviewing the available self-assessment NIST 800-171 tools. This process identified many shortcomings with the available tools and documentation that were addressed with the Dashboard. A few of these shortcomings included the following:

- Although there is a wealth of documentation, the sheer volume of information is extremely difficult to sort through, making it difficult for the non-expert to know where to begin;
- Specific implementation in guidance such as best practices and policy templates are not generally available;
- Many of the tools do not posture an organization for ongoing cyber security, nor establish a common framework or communication protocol on which to build their cyber security policies;
- The capability of an organization to share or communicate their cyber security posture, procedures, and artifacts with others in and outside the organization is difficult and/or costly; and,
- A centralized repository or portal where all affected and responsible parties can view, provide, or modify the data is not available.

With this background assessment, a series of conceptual design studies were conducted to identify the functions and capabilities that would be of greatest value to small and medium sized manufacturing organizations. From these studies, the requirements and prototype design for the Dashboard were developed. And, given the set of requirements, a cloud based solution was determined to be the best approach.

Next, detailed requirements, functional capabilities, and mockups were developed. An example set of requirements and a prototype mockup are shown below.

Table 1. Example set of requirements developed for the Dashboard.

#	Title	User Story	Description

1	Registration	Registration for individual users and organizations	• Individual users not associated with an organization
			  ○ User profile
			  ○ Payment method
			  ○ Include ability to switch between organizations and personal account
			• Organizational user
			  ○ Separate registration from user registration
			  ○ Admin will send invites to individual users to join
			  ○ One or more administrators should be accommodated
			  ○ The administrator(s) can add/remove individual users
			  ○ Payment method - only applies to organization
			  ○ The administrator(s) can specify a minimum password complexity for all users
			• Every user will have an unique username (email address)
			• Every user must have a password

2	Login	User must login before being able to access the Dashboard and their user profiles	• Reset password • Change password • Change profile • Change email address • Switch organization

3	Profile	Create a user profile	• Name (first, [middle], last)
			• Phone
			• email
			• Title/position per organization
			• Set of Roles per organization
			  ○ MVP (User/Admin)
			  ○ Post-MVP (Read/Write based on roles)

4	Payment system	A credit card payment system must be implemented	• Payment system is only required for Heartland's cloud solution • Detach payment system from docker instances distributed to end users • Credit Card (required) • ACH (if possible)
5	Home page	A home page with registration and login links	

6	Dashboard	A Dashboard page - the login landing page	
7		The Dashboard table should be modular	• Each cell in the Dashboard table should be a "module" that can be modified according to view and filter settings of the user. • The modules should be discoverable and modifiable
8		The Dashboard shall support multiple views	• The primary and only view required for the MVP is the NIST Cybersecurity Framework (draft-cybersecurity-framework-v1.1.pdf) • Post MVP views will include NIST SP 800-171 (NIST.SP.800-171r1.pdf), NIST SP 800-53 (NIST.SP.800-53r4.pdf), and NIST Manufacturing Profile (Manufacturing-Profile-DRAFT.pdf)
9		Map the NIST SP 800-171 (NIST.SP.800-171r1.pdf) controls to the cybersecurity framework	• For instances where there is not a direct mapping, select the most suitable functional area
10		Cross link all documents	• Every table entry in the Dashboard shall be hyperlinked to the appropriate document and section • All references in a document shall be hyperlinked
11	Docker implementation	A docker container will be the primary (only?) cloud-based implementation	• All site-specific parameters will be maintained outside of the docker container and source repository, e.g., email servers, ports, bank account information, etc.
12	Popup References	Hyperlinks in the Dashboard that reference passages from a document (i.e., the NIST 800-171, 800-53, Cybersecurity Framework, or Manufacturing profile) shall be displayed in a popup window (or something similar)	• When the document references are displayed, the popup window should include both the reference and an index (along the left side of the popup window) with links to each section of the document that is being referenced. • Only one section of the document should be displayed at a time. • The sections of the document are detailed in Database Requirements.

13	User customization	The user should be able to configure the base layer to match their particular risks and objectives	• Each user should be able add and remove elements from the Dashboard base layer
14	Point of Contact	The person responsible for each individual control should be identified in the Dashboard	• For each control, add a data field to capture the POC or person responsible for implementing the control

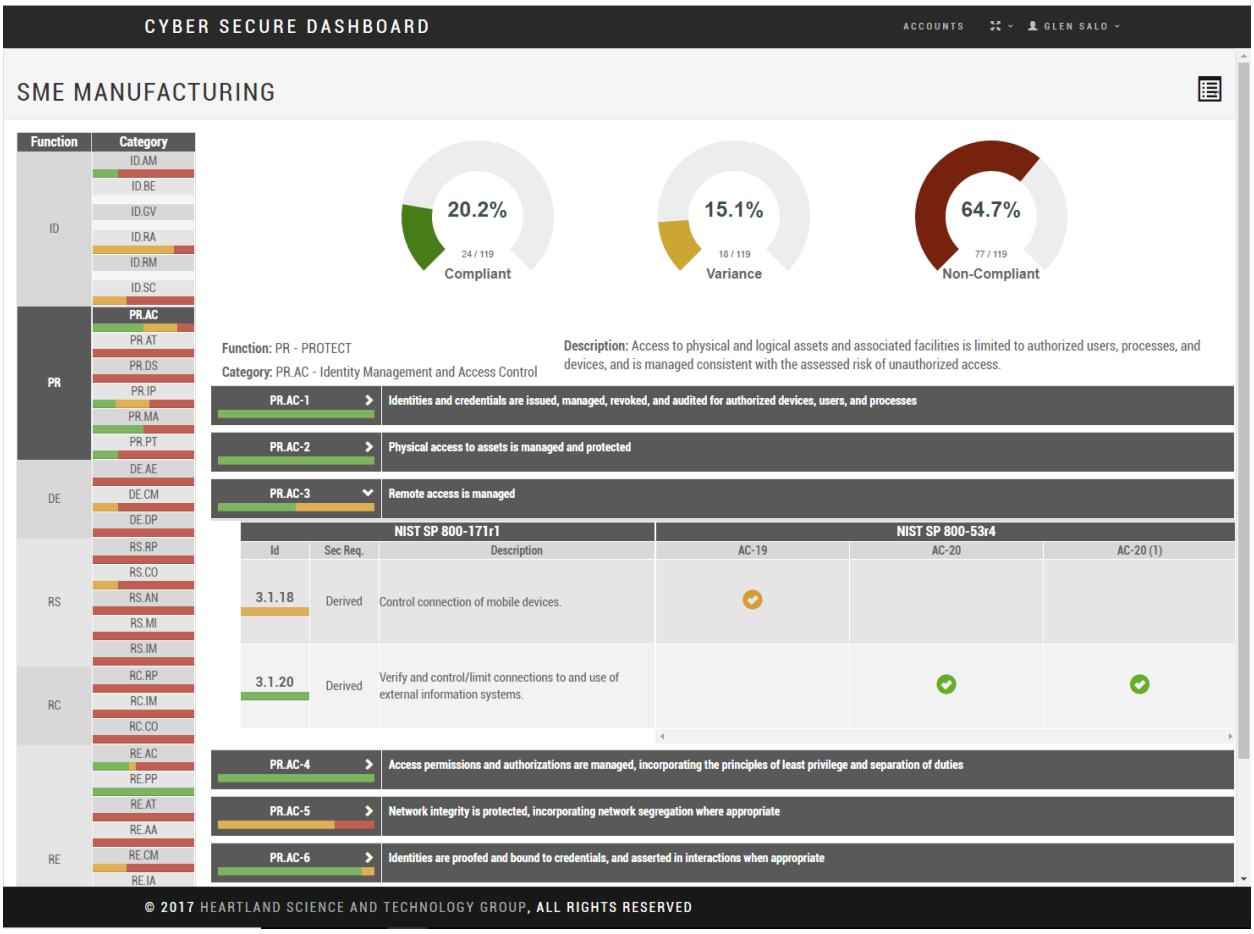


Figure 1. Actual screenshot of the Dashboard showing requirements and controls associated with "Identity Management and Access Control" under NIST CSF Function "Protect".

Given the requirements and the availability of existing background intellectual property developed by Heartland, the decision was made to leverage the existing software and to develop the Dashboard on the MEAN (MongoDB, express, AngularJS, and Node.js) stack foundation.

g. Users & Use Cases

The intent of this system is to assist organizations in complying with DFAR 252.204-7012 and the NIST SP 800-171r1, which is the primary use case. A secondary use case is for IT service providers that employ the Dashboard to support their client's need or desire to comply with the DFAR and NIST requirements. In either case, the operation of the Dashboard is nearly identical, the only difference being the number of accounts (i.e., Dashboards) created. Typically, an organization will create one account, or perhaps one account for each facility, whereas an IT service provider will create one (or more) accounts for each of their clients.

In both cases, the users of the Dashboard may include IT service provides, internal IT staff, other corporate employees, executives, prime contractors, subcontractors, insurance agents, and so forth. The cloud-based design of the Dashboard was specifically selected to support an unlimited number of users, within and without the organization, since everyone within the organization is impacted by cyber security and contributes to the overall cyber security of an organization.

IV. ACCESSING THE TECHNOLOGY

a. Background Intellectual Property

The Dashboard was built using background intellectual property developed by Heartland for two cloud based software projects.

b. Technical and Systems Requirements

The Dashboard technical and systems requirements are those of a typical cloud based dynamic website as summarized in Section III.b. While a working knowledge of computer system networking, and Docker containers is required to install, operate, and maintain the Dashboard, the Dashboard is available to everyone at http://www.cybersecureDashboardcybersecuredashboard.com.

V. INDUSTRY IMPACT & POTENTIAL

Although the primary objectives of the project were to address the needs of SME manufacturers subject to the DFARS requirements, the team has pursued a larger objective – to improve the cyber security and resilience of the entire US manufacturing base. The strategy to achieve this larger objective was to develop and deploy a simple, low-cost management tool that would ease and accelerate adherence to the NIST Cyber Security Framework cyber risk management process for all manufacturing firms – not just those subject to the DFARS.

Under a project separately funded by the Department of Homeland Security, the Critical Infrastructure Resilience Institute at the University of Illinois is currently adapting the Dashboard to support the NIST CSF Manufacturing Profile. As a part of this DHS grant, UIUC will also be conducting a workshop in the spring of 2018 to convene key representative stakeholders including prime contractors, SMMs, cyber

insurance industry, and government to consider the potential for enhancing the security and resilience of the manufacturing sector through adherence to standardized cyber risk management processes.

According to the National Association of Manufacturers, there are over 250,000 manufacturing firms in the US – most of which are small/medium enterprises – employing 12.3 million workers.

Potential Market Impact

We believe that – given its cloud-based design, ease of use, and integration of both the 800-171 requirements and the NIST Cyber Security Framework - the Dashboard has the potential to become a widely used *platform* for cyber risk management within SMEs and large companies in manufacturing and many other industrial sectors.

It is our belief that a standardized platform for cyber risk management is necessary for a number of reasons. First of all, it must be acknowledged that sound cybersecurity is not a one-time, one-and-done exercise. Rather, given the constantly evolving threat and technology landscapes, cybersecurity is an ongoing process that requires constant focus and effort. In addition, sound cyber risk management involves the entire corporation – with particular emphasis on the active engagement of upper management. A standardized platform accessible to all participants is necessary to maintain organization-wide engagement. Lastly, given the market forces discussed above, we would assert that *standardization* of cyber risk management processes will become a business necessity.

[Appropriately addressing business risk is a primary function of corporate management. Financial losses associated with cyber breaches are steadily rising across all industries making cyber risk an increasingly significant element of overall business risk. Risk and casualty insurance is a primary mechanism used by businesses to address and reduce business risk.

From research being conducted at UIUC it has been noted that a widespread impediment to maturity of the cyber insurance market centers on the inability of insurers to accurately assess the underwriting risk associated with a potential insured organization. As a result, cyber insurers are pricing their risk uncertainty into premiums (resulting in more cost to the insured) and including numerous exclusions in their policies (increasing the financial risk to the insured). Insurers simply do not have the capability or willingness to individually assess the cybersecurity posture and/or cyber risk management practices of every potential insured. Accordingly, we believe the insurance industry will demand that potential insured companies adopt and maintain recognizable, *standardized* cyber risk management processes. Adherence to *standardized* cyber risk management processes (and *standardized* underlying security controls) will allow insurers to gauge the relative underwriting risk of potential insured companies in terms of their relative compliance/conformance to the standard. Given that the NIST CSF represents just such a *standardized* cyber risk management process we believe that it will become a de facto requirement to obtain affordable and effective cyber insurance in the future.

Integration of the NIST CSF is a core design feature of the Dashboard which we believe directly addresses the needs of cyber insurers for just such a *standardized* cyber risk management process and which will propel the uptake of the Dashboard within the manufacturing industry and others. Therefore, the introduction and broad uptake of the Dashboard could – through its potential to reduce cyber insurance premiums – deliver many millions of dollars of cost savings to the manufacturing sector.]

VI. ASSESSMENT RESULTS

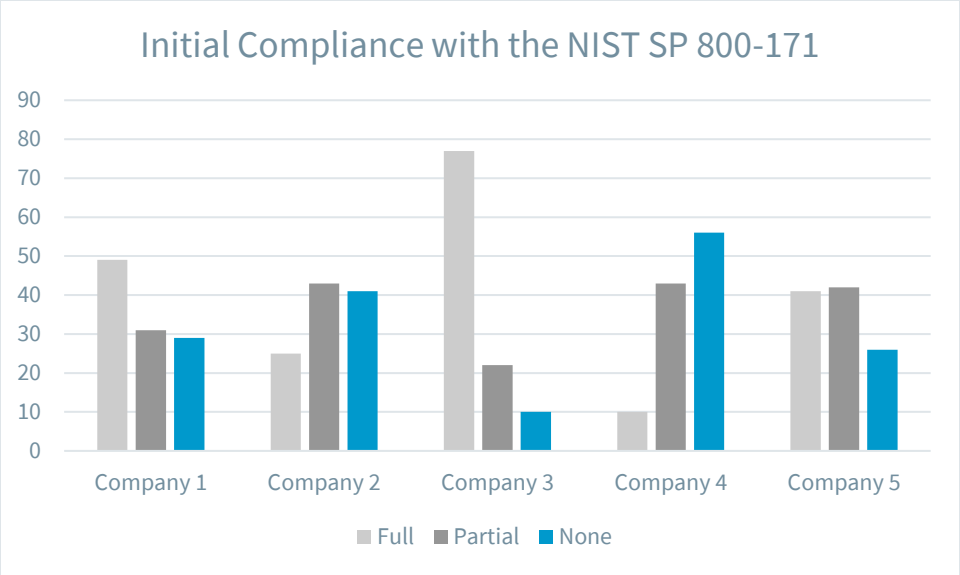
In addition to creating the dashboard, the project team assessed five small to medium-sized manufacturing organizations. The assessments consisted of a pre-assessment survey, an in-person meeting with corporate representatives responsible for IT security (executives and senior managers, and IT staff and consultants), and a post beta-test survey. The in-person meetings focused on going through the NIST SP 800-171r1 controls one-by-one to ascertain the status of each organization, whereas the surveys collected general information regarding each organization's understanding of the requirements, their preparedness, their estimated level of effort and cost to become compliant, and their feedback on the Dashboard.

The five steps any organization has to take to become minimally compliant with the DFARS are listed below. Our assessment focused on conducting a GAP analysis (the first step) and providing the organizations with templates and other information they could utilize in their efforts to satisfy the remaining steps.

1) Performing a GAP analysis considering current state vs NIST 800-171/53 (see table below);
2) Preparing and implementing policies (utilize policy templates provided in the Dashboard);
3) Implementing security controls (using Dashboard to cross reference to NIST 800-53); internally validate;
4) Implementing a training program to include Security Awareness; and
5) Implementing a network security monitoring solution that provides for alerting and reporting on anomalous activity, as well as regularly scheduled vulnerability scans.

The results of our assessment for the five organizations is summarized in the table and figure below. From this data, it can quickly be ascertained that, with the exception of one company, these organizations have a lot of work to do before they are DFARs compliant. Company 3 was the most compliant with 77 of 109 controls fully implemented, whereas Company 4 was the least compliant with only 10 controls fully implemented and 56 controls non-compliant.

Status	Company 1	Company 2	Company 3	Company 4	Company 5
Fully compliant	49	25	**77**	10	41
Partially compliant	31	43	22	43	42
Not compliant	29	41	10	**56**	26
Total	109	109	109	109	109



An investigation of the commonality of the controls implemented between the five organizations revealed (surprisingly) very little overlap. For example, out of the 109 controls, there were only 5 common controls that each organization had implemented.

Common Fully Compliant Controls

- 3.1.15 – Authorize remote execution of privileged commands and remote access to security-relevant information.
- 3.1.22 – Control information posted or processed on publicly accessible information systems.
- 3.5.11 – Obscure feedback of authentication information.
- 3.14.4 – Update malicious code protection mechanisms when new releases are available.
- 3.14.5 – Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Similarly, the organizations had only 4 common controls that were non-compliant and 2 common controls that were partially compliant as summarized below.

Common Partially Compliant Controls

- 3.5.4 – Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
- 3.11.2 – Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.

Common Non-Compliant Controls

- 3.1.11 – Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.
- 3.6.3 – Test the organizational incident response capability.

- 3.8.8 – Prohibit the use of portable storage devices when such devices have no identifiable owner.
- 3.13.11 – Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

The team also assessed the commonality of the controls when only any 3 of the 5 organizations were in agreement for any particular control. Using this criterion, the number of common controls increased to 36, 23, and 25 for compliant, partially compliant, and non-compliant, respectively. This result reinforces the conclusion that there is little commonality between the organizations, particularly since the 3 organizations in agreement can change for each control.

This lack of similarity suggests that the organizations do not prioritize the controls in the same order and that their security posture is highly dependent upon the knowledge and practices of the IT personal implementing the controls. This observation emphasizes the need for a tool to guide the corporations through the process of securing their IT systems.

Similarly, the estimated costs provided by the organizations to gain an understanding of the requirements, implement the controls, and train their personnel varied greatly as summarized below. This result once again suggests a general deficiency in understanding the requirements and the steps required to implement the security controls, which further suggests that a tool that provides the required knowledge base and detailed implementation guidance is needed.

- Estimated cost to determine the requirements: $2K – $150K.
- Estimated cost to implement the controls: $5K – $500K.
- Estimated cost to train personnel: $5K – $500K.

The estimated costs associated with the five steps to become minimally compliant for HL Precision Manufacturing is summarized below:

1) GAP Analysis - $4,500 – 24 hours of professional service of a Security Advisor, familiar with the SME environment;
2) Policy Creation – $4,000 – Professional service to adapt policies for SME approval and adoption by SME management, followed by staff orientation and training;
3) Controls implementation - $8,000 – Professional service for mitigation of “critical” and “high” vulnerabilities identified during vulnerability scan performed during GAP Analysis;
4) Training Program - $4,200/year – Security Awareness Program implemented, considers annual in-person training of all staff, email phishing tests, security awareness email alerts, and signage;
5) Security Monitoring - $4,800/year – Utilizing a network monitoring appliance which monitors and sends daily alerts on Anomalies, Changes, and Threats (ACT). Service also includes automated vulnerability scans performed weekly, with monthly reporting on vulnerabilities and changes in security posture.

TOTAL 1ST YEAR: $25,500

TOTAL/YEAR THEREAFTER: $9,000

*We expect these costs are lower than what other SME’s might incur due to ongoing relationship that this specific SME has with a full service managed IT services provider.

Next Steps

Following the project timeframe, controls will be implemented for external media devices and to address shop-floor situations where generic user accounts are utilized on kiosk systems. A draft three-year plan is being considered that prioritizes system upgrades that will address the controls necessary to mitigate additional risks, such as data encryption at rest and to enable secure wireless access to internal network resources.

VII. TECH TRANSITION PLAN & COMMERCIALIZATION

The Dashboard technology and product is being transitioned to a for-profit entity that will commercialize and support the product in the broad market for cyber security risk management tools. Technology license discussions/negotiations are underway.

Under a grant from the Department of Homeland Security the team is currently adapting the Dashboard to support the NIST CSF Manufacturing Profile and has plans to also support the Bulk Liquids Transfer Profile, the soon-to-be-released Passenger Vessel Profile, and other CSF Profiles as they are released by NIST.

VIII. WORKFORCE DEVELOPMENT

The Dashboard presents cyber security requirements in the NIST CSF format which educates and reinforces the NIST CSF cyber risk management process – thus developing a more knowledgeable and cyber risk-aware workforce.

Additionally, the Dashboard contains detailed “Best Practices” for each security control (from NIST 800-53) that is specified or referenced in the DFARS/NIST 800-171. These Best Practices “interpret” the NIST 800-53 control requirements into language familiar to any competent IT or management professional and describes *how* a security control needs to be implemented.

Simply by providing this mapping of NIST 800-53 security control requirement to specific “Best Practices” the Dashboard helps educate IT and management professionals on the security control requirements and sound implementation guidelines. In other words, the integrated “Best Practices” allow IT and management professionals to “learn by doing”: as they address the DFARS using the Dashboard they are learning the specific details of the compliance requirements as well as how the requirements must be met and maintained.

IX. CONCLUSIONS/RECOMMENDATIONS

The team was able to deliver a product that has received strongly positive reviews from a wide range of constituents in the manufacturing domain. Having successfully completed a beta test program the product is being delivered to DMDII Members as per the terms of the research grant.

Although the team believes that the product can have a significant and positive impact on the cyber security and resilience of the manufacturing sector its impact will, by definition, be determined by the product's commercial market success.

The team recommends that – within the bounds of its legal and contractual obligations – DMDII reinforce to its membership base and the larger manufacturing community the importance of achieving and sustaining heightened cyber security through compliance with the DFARS and/or adherence to NIST CSF standards and to advise that same audience of the availability of the Dashboard and other products that can assist manufacturers in achieving compliance with the DFARS and otherwise enhancing their cyber security posture.

X. Requested Enhancements

The following list comprises the enhancements requested by our beta testers. Please note that this list does not include minor cosmetic or functionality enhancements and that all of these requests have either been implemented or are scheduled for implementation in the near term.

1. Add a perpetual "Welcome, Account_User_Name" at the top of the page to allow the person using the tool to assure that they are logged in regardless of where navigating takes them.
2. Identify the minimum requirement controls
3. Within each control, under the assessment section, it would be good to be able to indicate more fidelity besides just "non-compliant" or "variance". For example, we have many controls where we are mostly compliant, but we have a few tasks to accomplish to get fully compliant. It would be nice to be able to get a sense from the dashboard how far away you are form compliant, or the magnitude of the amount of work left to get to compliance. Possible additional data fields:
    a. Percent compliant
    b. Expected compliance date
    c. Estimated labor hours to compliance
4. Would be great to have some export options. For example, an option to export all compliance assessment descriptions as a single document, listing artifacts as supplemental documentation (not exporting each artifact necessarily, just a reference to it)
5. It would be nice to be able to search within the data. For example, I think I remember there is a requirement for a consistent time server but I don't remember where it is located. It would be nice to search instead of having to click through individual items to find it again.
6. When two or more users are on the same page, and one makes a change, the others should be notified.
7. Provide a recommended path of compliance. For example, taking care of control "X" will make satisfying the rest of the controls much easier and should be completed first. Enable the creation of prioritization tables, the above being one choice. Others may be user defined, such as given by a prime contractor or the insurance agent.
8. Toggle to show / hide the gray area of controls. Add an according (or similar) feature that lets the user collapse the Cyber Secure Framework descriptions when not needed.
9. Ability to prevent users from uploading files to SAAS site (and other functions).
10. Show status of invitees as pending, accepted, etc. Also show date / time of last login.

11. Have the left pane filter / show the different requirements sorted by the requirement. currently follows CSF. Would be nice to have an option that follows NIST 800-171 in the order it is written. This will help people who are familiar with one but not the other.
12. Add a verification checkbox to each assessment. To be used as a manager or second signoff (with who and when recorded).
13. To be used as a manager or second signoff (with who and when recorded). Key information: Who signed off and when; complete toward compliance.